



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,981	09/12/2003	Kevin Moore	60046.0052US01	6124

7590 08/24/2007
Hope Baldauff Hartman, LLC
Suite 1010
1720 Peachtree Street
Atlanta, GA 30309

EXAMINER

REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

08/24/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/660,981	Applicant(s) MOORE, KEVIN	
	Examiner Mohammad W. Reza	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) 1-21 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the arguments filed on 07/05/2007.
2. Claims 1-21 are pending in the application.
3. Claims 1-21 have been rejected.

Response to Arguments

5. Applicant's arguments filed on 07/05/2007 have been fully considered but they are not persuasive.

For independent claim 1, applicant argues that Kodama does not disclose "determining from the data storage device identifiers whether the data storage device supports the security features".

Examiner respectfully disagrees. For example, "the host computer comprising: storage means for storing a host ID of the host computer; password number input means for admitting a password number corresponding to the host ID; element information input means for admitting element information designating at least one element on which the command is to be executed; command type input means for admitting a command type indicating at least whether the command is a security protection locking command or a security protection unlocking command; command generation means for generating the command by formatting the host ID, the password number, the element information, and the command type into a suitable format; and output means for outputting the command to the changer apparatus (col. 2, lines 19-32) discloses

Art Unit: 2136

this limitation. Applicant argues that Kodama does not teaches "determining wheter the data storage device is locked and returning from a powered off state or a hardware reset". Examiner respectfully disagrees. For example, "the security protection locking method comprising the steps of: admitting a command from a host computer furnished externally; verifying whether the command received from the host computer is a security protection locking command; if the command from the host computer is found to be a security protection locking command, verifying whether element information included in the security protection locking command to designate an element on which security protection is to be locked overlaps with element information included in the security protection information stored in the storage means; and if the two kinds of element information are found not to overlap with each other, storing into the storage means a host ID of the host computer, a password number corresponding to the host ID, the element information included in the security protection locking command, and a restricted range in which commands from the host computer are executed (col. 3, lines 1-17), and "the security protection unlocking method comprising the steps of: admitting a command from a host computer furnished externally; verifying whether the command received from the host computer is a security protection

Art Unit: 2136

unlocking command; if the command from the host computer is found to be a security protection unlocking command, verifying whether a host ID of the host computer coincides with a host ID in the security protection information stored in the storage means; if the host ID of the host computer and the host ID in the security protection information stored in the storage means are found to coincide with each other, verifying whether a password number included in the security protection unlocking command coincides with a password number in the security protection information (col. 3, lines 31-45) discloses this limitations. Further, applicant argues that, "Kodama does not disclose "in response to determining that the data storage device is locked and returning from a powered off state or a hardware reset, receiving from a user a password fro unlocking the data storage device". Examiner respectfully traverses this argument. "The storage means such as a nonvolatile memory stores information about security protection that is locked on such elements as compartments in the medium rack and the drive. When security protection is to be locked, the system controller is supplied with a security protection locking command from the outside. Under control of the system controller, security protection information is written to the nonvolatile memory. The security protection information comprises illustratively a host

Art Unit: 2136

ID, a password number, a security level, and a group of elements selected from such components as the compartments in the medium rack and the drive. When security protection is to be unlocked, the system controller is supplied with a security protection unlocking command from the outside. Under control of the system controller, applicable security protection information is erased from the nonvolatile memory (col. 4, lines 34-49), "Suppose that the system controller 110 is supplied with the security protection locking command (with bit 0 of byte 10 set for 1) shown in FIG. 5. In that case, the system controller 110 locks security protection on the selected group of elements except when part or all of the elements overlap with those on which security protection has already been locked. As illustrated in FIG. 6, the nonvolatile memory 114 stores, as security protection information, host IDs of host computers having supplied security protection locking commands to the system controller, password numbers of the host computers, element groups each designated by a starting address and an element count, and security levels. Suppose now that the system controller 110 is supplied with the security protection unlocking command (with bit 0 of byte 10 set for 0) shown in FIG. 5. In such a case, if the host ID, password number and element group set in the security protection unlocking command

Art Unit: 2136

coincide with any ID, password number and element group in the security protection information in the nonvolatile memory 114, then the system controller 110 erases the applicable pieces of security protection information from the nonvolatile memory 114 (col. 7, lines 45-67) disclose this limitation.

Dependent claims 1-14 are also rejected due their dependency on independent claim 1. However, Kodama also discloses the teachings of "a power on test procedure of a computer hosting the data storage devices". "Conventional changer apparatuses do not have security protection features. Such a changer apparatus lets all recording media therein be accessed from any host computer which can readily read data from the media. Although the SCSI has reserve commands, reserved information is released when power is turned off or when a reset signal is input. The turning-off of power or the input of the reset signal is accomplished regardless of a host computer having reserved information in the change apparatus (col. 1, lines 36-45), and "Host IDs, password numbers, security levels, element groups whose security is to be protected, and other security-related information are written to or erased from the nonvolatile memory 114. In executing commands from host computers, the system controller 110 references the stored security protection information so as to protect data security within the changer apparatus 100. When power is removed, the security protection information remains stored. Because unlocking of security protection requires the matching of password numbers, the internal data in the changer apparatus 100 is securely protected. In addition, the security level and the elements whose security is to be protected may be set as desired in order to address varieties of applications (col. 9, lines 20-33) discloses this limitation.

Examiner also found that Kodama discloses the limitation of claim 3, "preparing each locked data storage device for provided to each locked data storage device", "preparing each locked data storage device for presentation to an operating system fro limited access", and "isolating each locked data storage device from the operating system". For example, "In the above constitution, suppose that a command from any one of the host computers 140-1 through 140-Q is supplied through the SCSI bus 150 to the system controller 110 of the changer apparatus 100. In such a case, the system controller 110 refers to security

Art Unit: 2136

protection information in the nonvolatile memory 114 to control the execution of the command. Illustratively, if the command from the host computer is one for gaining access to an element (any of the cassette rack 101, tape drivers 102-1 through 102-P, tape cassettes, etc.) whose security is protected against such attempted command execution, the system controller 110 rejects the execution of that command. Security protection of the changer apparatus 100 is locked (or unlocked) by any of the host computers 140-1 through 140-Q supplying a security protection locking (or unlocking) command via the SCSI bus 150 to the system controller 110 of the changer apparatus 100". "According to another aspect of the invention, there is provided a host computer for use with a changer apparatus comprising a medium rack having a plurality of compartments for accommodating recording media, at least one drive for gaining access to the recording media, recording medium transfer means for transferring the recording media between the medium rack and the drive, storage means for storing security protection information by which to ensure security protection of the changer apparatus, command input means for admitting an externally input command, and a system controller for controlling execution of the command entered through the command input means in accordance with the security protection information stored in the storage means, the host computer outputting the command to the changer apparatus, the host computer comprising: storage means for storing a host ID of the host computer; password number input means for admitting a password number corresponding to the host ID (col. 2, lines 5-25), and "Suppose that the system controller 110 is supplied with the security protection locking command (with bit 0 of byte 10 set for 1) shown in FIG. 5. In that case, the system controller 110 locks security protection on the selected group of elements except when part or all of the elements overlap with those on which security protection has already been locked. As illustrated in FIG. 6, the nonvolatile memory 114 stores, as security protection information, host IDs of host computers having supplied security protection locking commands to the system controller, password numbers of the host computers, element groups each designated by a starting address and an element count, and security levels. Suppose now that the system controller 110 is supplied with the security protection unlocking command (with bit 0 of byte 10 set for 0) shown in FIG. 5. In such a case, if the host ID, password number and element group set in the security protection unlocking command coincide with any ID, password number and element group in the security protection information in the nonvolatile memory 114, then the

Art Unit: 2136

system controller 110 erases the applicable pieces of security protection information from the nonvolatile memory 114 (col. 7, lines 45-67) disclose this limitation

Kodama discloses the limitation of claim 5 as well. "As described and according to the invention, security protection information is stored illustratively in a nonvolatile memory. The information is referenced by the controller that controls the execution of commands coming from host computers. When power is turned off, the stored information remains intact and serves as the basis for protecting security of data within the changer apparatus. With passwords used as part of the security protection information, security protection is unlocked only upon coincidence of a stored and a subsequently supplied password number. This ensures higher levels of data security protection than before. Furthermore, varieties of applications may be addressed where a desired group of elements whose security is to be protected and a preferred security level are set as part of the security protection information" discloses the limitation of claim 5.

Kodama discloses the limitation of claim 6. For example, ". "As described and according to the invention, security protection information is stored illustratively in a nonvolatile memory. The information is referenced by the controller that controls the execution of commands coming from host computers. When power is turned off, the stored information remains intact and serves as the basis for protecting security of data within the changer apparatus. With passwords used as part of the security protection information, security protection is unlocked only upon coincidence of a stored and a subsequently supplied password number. This ensures higher levels of data security protection than before. Furthermore, varieties of applications may be addressed where a desired group of elements whose security is to be protected and a preferred security level are set as part of the security protection information", and "The storage means such as a nonvolatile memory stores information about security protection that is locked on such elements as compartments in the medium rack and the drive. When security protection is to be locked, the system controller is supplied with a security protection locking command from the outside. Under control of the system controller, security protection information is written to the nonvolatile memory. The security protection information comprises illustratively a host ID, a password number, a security level, and a group of elements selected from

Art Unit: 2136

such components as the compartments in the medium rack and the drive. When security protection is to be unlocked, the system controller is supplied with a security protection unlocking command from the outside. Under control of the system controller, applicable security protection information is erased from the nonvolatile memory" discloses this feature of the claim.

Kodama discloses the limitation of claim 9-11. For example, "As described and according to the invention, security protection information is stored illustratively in a nonvolatile memory. The information is referenced by the controller that controls the execution of commands coming from host computers. When power is turned off, the stored information remains intact and serves as the basis for protecting security of data within the changer apparatus. With passwords used as part of the security protection information, security protection is unlocked only upon coincidence of a stored and a subsequently supplied password number. This ensures higher levels of data security protection than before. Furthermore, varieties of applications may be addressed where a desired group of elements whose security is to be protected and a preferred security level are set as part of the security protection information", "As described and according to the invention, security protection information is stored illustratively in a nonvolatile memory. The information is referenced by the controller that controls the execution of commands coming from host computers. When power is turned off, the stored information remains intact and serves as the basis for protecting security of data within the changer apparatus. With passwords used as part of the security protection information, security protection is unlocked only upon coincidence of a stored and a subsequently supplied password number. This ensures higher levels of data security protection than before. Furthermore, varieties of applications may be addressed where a desired group of elements whose security is to be protected and a preferred security level are set as part of the security protection information", and "The storage means such as a nonvolatile memory stores information about security protection that is locked on such elements as compartments in the medium rack and the drive. When security protection is to be locked, the system controller is supplied with a security protection locking command from the outside. Under control of the system controller, security protection information is written to the nonvolatile memory. The security protection information comprises illustratively a host ID, a password number, a security level, and a group of elements selected from

Art Unit: 2136

such components as the compartments in the medium rack and the drive. When security protection is to be unlocked, the system controller is supplied with a security protection unlocking command from the outside. Under control of the system controller, applicable security protection information is erased from the nonvolatile memory" discloses these features of the claim.

Kodama discloses the limitation of claims 12, 13, 16, and 17. "preparing each locked data storage device for provided to each locked data storage device", "preparing each locked data storage device for presentation to an operating system fro limited access", and "isolating each locked data storage device from the operating system". For example, "In the above constitution, suppose that a command from any one of the host computers 140-1 through 140-Q is supplied through the SCSI bus 150 to the system controller 110 of the changer apparatus 100. In such a case, the system controller 110 refers to security protection information in the nonvolatile memory 114 to control the execution of the command. Illustratively, if the command from the host computer is one for gaining access to an element (any of the cassette rack 101, tape drivers 102-1 through 102-P, tape cassettes, etc.) whose security is protected against such attempted command execution, the system controller 110 rejects the execution of that command. Security protection of the changer apparatus 100 is locked (or unlocked) by any of the host computers 140-1 through 140-Q supplying a security protection locking (or unlocking) command via the SCSI bus 150 to the system controller 110 of the changer apparatus 100", "According to another aspect of the invention, there is provided a host computer for use with a changer apparatus comprising a medium rack having a plurality of compartments for accommodating recording media, at least one drive for gaining access to the recording media, recording medium transfer means for transferring the recording media between the medium rack and the drive, storage means for storing security protection information by which to ensure security protection of the changer apparatus, command input means for admitting an externally input command, and a system controller for controlling execution of the command entered through the command input means in accordance with the security protection information stored in the storage means, the host computer outputting the command to the changer apparatus, the host computer comprising: storage means for storing a host ID of the host computer; password number input means for admitting a password number corresponding to the host ID (col. 2, lines 5-25), and "Suppose that the system controller

Art Unit: 2136

110 is supplied with the security protection locking command (with bit 0 of byte 10 set for 1) shown in FIG. 5. In that case, the system controller 110 locks security protection on the selected group of elements except when part or all of the elements overlap with those on which security protection has already been locked. As illustrated in FIG. 6, the nonvolatile memory 114 stores, as security protection information, host IDs of host computers having supplied security protection locking commands to the system controller, password numbers of the host computers, element groups each designated by a starting address and an element count, and security levels. Suppose now that the system controller 110 is supplied with the security protection unlocking command (with bit 0 of byte 10 set for 0) shown in FIG. 5. In such a case, if the host ID, password number and element group set in the security protection unlocking command coincide with any ID, password number and element group in the security protection information in the nonvolatile memory 114, then the system controller 110 erases the applicable pieces of security protection information from the nonvolatile memory 114 (col. 7, lines 45-67) disclose this limitation

Kodama discloses the limitation of claims 18, 19, and 20. For example, "As described and according to the invention, security protection information is stored illustratively in a nonvolatile memory. The information is referenced by the controller that controls the execution of commands coming from host computers. When power is turned off, the stored information remains intact and serves as the basis for protecting security of data within the changer apparatus. With passwords used as part of the security protection information, security protection is unlocked only upon coincidence of a stored and a subsequently supplied password number. This ensures higher levels of data security protection than before. Furthermore, varieties of applications may be addressed where a desired group of elements whose security is to be protected and a preferred security level are set as part of the security protection information", "As described and according to the invention, security protection information is stored illustratively in a nonvolatile memory. The information is referenced by the controller that controls the execution of commands coming from host computers. When power is turned off, the stored information remains intact and serves as the basis for protecting security of data within the changer apparatus. With passwords used as part of the security protection information, security protection is unlocked only upon coincidence of a stored and a subsequently supplied password

Art Unit: 2136

number. This ensures higher levels of data security protection than before. Furthermore, varieties of applications may be addressed where a desired group of elements whose security is to be protected and a preferred security level are set as part of the security protection information", and "The storage means such as a nonvolatile memory stores information about security protection that is locked on such elements as compartments in the medium rack and the drive. When security protection is to be locked, the system controller is supplied with a security protection locking command from the outside. Under control of the system controller, security protection information is written to the nonvolatile memory. The security protection information comprises illustratively a host ID, a password number, a security level, and a group of elements selected from such components as the compartments in the medium rack and the drive. When security protection is to be unlocked, the system controller is supplied with a security protection unlocking command from the outside. Under control of the system controller, applicable security protection information is erased from the nonvolatile memory" discloses these features of the claim.

Kodama also discloses the limitations of claims 4, 7, 8, 15, and 21 as well.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Kodama et al hereafter Kodama (US patent 5983349).

7. As per claim 1, 14, and 15 Kodama discloses a method comprising: reading from each of the data storage devices one or more data storage device identifiers;

Art Unit: 2136

determining from the data storage device identifiers whether the data storage device supports the security features; in response to determining that the data storage device supports the security features, determining whether the data storage device is locked and returning from a powered off state or a hardware reset (col. 2, lines 5-33); in response to determining that the data storage device is locked and returning from a powered off state or a hardware reset, receiving from a user a password for unlocking the data storage device; in response to receiving the password, determining whether the received password is the security password; and in response to the received password being the security password, unlocking the data storage device and thereby allowing access to data stored on the data storage device (col. 3, lines 17-55).

8. As per claim 2, Kodama discloses the method wherein the method is implemented during a power on test procedure of a computer hosting the data storage devices (col. 4, lines 34-49).

9. As per claim 3, Kodama discloses the method comprising: in response to the data storage device remaining locked, determining whether limited access should be provided to each locked data storage device; in response to determining that limited access should be provided, preparing each locked data storage device for presentation to an operating system for limited access; and in response to determining that limited access should not be provided to each locked data storage device, isolating each locked data storage device from the operating system (col. 2, lines 55-67, col. 3, lines 1-17).

Art Unit: 2136

10. As per claim 4, Kodama discloses the method wherein limited access comprises prohibiting reading from or writing to the locked data storage device (col. 2, lines 55-67, col. 3, lines 1-17).

11. As per claim 5, Kodama discloses the method wherein the data storage devices are locked upon experiencing a powered off state, a sleep state, or a hardware reset, and wherein the method further comprises: in response to the received password being the security password, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password; and in response to determining that the data storage device should be unlocked without requiring a user to enter a password, storing the security password within a memory located outside the data storage device (col. 2, lines 5-33, col. 1, lines 37-45).

12. As per claim 6, Kodama discloses the method comprising: in response to determining that the data storage device is locked, determining whether the data storage device is returning from a powered off sleep state; in response to the data storage device being locked and returning from a powered off sleep state, determining whether the data storage device was unlocked prior to the sleep state; in response to determining that the data storage device was unlocked prior to the sleep state, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password; and in response to determining that the data storage device should be unlocked without requiring a user to enter a password, retrieving the security password from the memory and utilizing the security password to unlock the data storage device (col. 2, lines 5-33, col. 1, lines 37-45).

13. As per claim 7, Kodama discloses the method wherein the security password is stored within the memory in an encrypted format (col. 2, lines 5-33).

14. As per claim 8, Kodama discloses the method comprising in response to determining that the data storage device should be unlocked after returning from a sleep state by requiring a user to enter a password, receiving the security password from a user and utilizing the security password to unlock the data storage device (col. 3, lines 17-55).

15. As per claim 9, Kodama discloses the method comprising: in response to determining that the data storage device is unlocked, determining whether a security password has been enabled; and in response to determining that the data storage device is unlocked and that no security password is enabled for the data storage device, disabling, until a next power cycle, the security features that enable security passwords (col. 2, lines 5-33, col. 1, lines 37-45).

16. As per claim 10, Kodama discloses the method comprising: in response to the data storage device being locked and returning from a powered off state or a hardware reset, determining whether a backup password may be used to unlock the data storage device; in response to determining that a backup password may be used; determining whether a request to enter a backup password has been received; in response to receiving a request to enter a backup password, receiving from a user a password for unlocking the data storage device; and in response to the received password being the backup password, unlocking the data storage device and thereby allowing access to data stored on the data storage device (col. 2, lines 5-33).

Art Unit: 2136

17. As per claim 11, Kodama discloses the method comprising: in response to the received password being the backup password, determining whether a maximum security is supported by the security features; and in response to the received password being the backup password and the maximum security being supported, erasing the data storage device before unlocking the data storage device (col. 2, lines 5-33).

18. As per claim 12, Kodama discloses the method wherein a password entry attempt counter is set for a maximum number of entry attempts allowed, further comprising: in response to determining that the password is not the security password, determining whether the password entry attempt counter is equal to zero; in response to the password entry attempt counter being greater than zero, decrementing the password entry attempt counter by one and again receiving a password from a user; and in response to the password entry attempt counter equaling zero, prohibiting additional password entries until a next power cycle and displaying a message that the data storage device remains locked (col. 2, lines 55-67, col. 3, lines 1-17).

19. As per claim 13, Kodama discloses the method comprising executing a setup utility within the basic input/output system operative to control one or more functions for manipulating at least one of a security password and a backup password for a data storage device supporting the security features wherein the functions are accessed by one of entering the security password when prompted by the setup utility and selecting the data storage device in the setup utility when said data storage device is unlocked (col. 2, lines 55-67, col. 3, lines 1-17).

20. As per claim 16, Kodama discloses a system for securing the contents of one or more data storage devices capable of storing a security password for unlocking and locking the data storage

devices located within a computer, the system comprising: a display; a memory; a central processing unit; a basic input/output system for controlling the basic input/output functions of the computer comprising an operating system independent setup utility for controlling functions for manipulating data storage device security (col. 2, lines 5-33).

21. As per claim 17, Kodama discloses the system wherein the operating system independent setup utility is operative to receive a selection of a data storage device, receive a selection of a password function to perform on the selected data storage device, determine whether a security password has been enabled for a selected data storage device, in response to the security password not being enabled, receive from a user a security password, and in response to receiving the security password from the user, enable the security password on the selected data storage device, wherein enabling the security password includes storing the security password on the selected data storage device thereby preventing access to contents of the selected data storage device when the selected data storage device is locked with the security password (col. 3, lines 17-55).

22. As per claim 18, Kodama discloses The system, wherein the operating system independent setup utility is further operative to determine whether a hardware reset is performed when the setup utility is exited and in response to determining that a hardware reset is not performed when the setup utility is exited, exit the setup utility and

Art Unit: 2136

remove power from the selected data storage device thereby locking the selected data storage device with the security password (col. 2, lines 5-33, col. 1, lines 37-45).

23. As per claim 19, Kodama discloses the system, wherein the operating system independent setup utility is further operative to one of: in response to the security password being enabled, receive a password from a user, in response to receiving a password, determine whether the password is the security password by attempting to disable security for the selected data storage device with the password, and in response to the received password being the security password, disable then re-enable the security of the selected data storage device thereby validating the password as the security password; and in response to the security password being enabled and the data storage device being unlocked, grant access to the functions for manipulating data storage device security (col. 2, lines 55-67, col. 3, lines 1-17).

24. As per claim 20, and 21 Kodama discloses a method comprising: storing a security password within a memory located outside the data storage device; in response to determining that the data storage device is locked, determining whether the data storage device is returning from a sleep state (col. 2, lines 5-33); in response to the data storage device being locked and returning from a sleep state, determining whether the data storage device was unlocked prior to the sleep state; and in response to determining that the data storage device was unlocked prior to the sleep state, retrieving the security password from the memory and utilizing the security password to unlock the data storage device (col. 3, lines 17-55).

Conclusion

25. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status


Art Unit: 2136

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


8/21/07